JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 17. juni 2025
Kontor: Kontoret for EU-ret og Databeskyttelse
Sagsbeh: Ane Caroline Meyer Nilsson
Sagsnr.: 2025-06642
Dok.: 3740392

Besvarelse af spørgsmål nr. 1135 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 1135 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 20. maj 2025. Spørgsmålet er stillet efter ønske fra ikkemedlem af udvalget (MFU) Peter Kofod (DF).

Peter Hummelgaard

/

Maria Aviaja Hesby Holm

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1135 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren som opfølgning på KUU alm. del - spørgsmål nr. 316 (2020-21) oplyse, om der er nogen forandring i reglerne fra Datatilsynet mv. i relation til brug af ansigtsscan ved betalingssystemer – f.eks. turbånd i forlystelsesparker? Vil ministeren desuden præcisere, hvilke regler der i disse situationer gælder for mindreårige – skal forældre give samtykke og i givet fald hvordan mv.? Og endelig bedes ministeren oplyse, hvor meget
> rum Folketinget har til at regulere disse spørgsmål, henset til at meget kommer fra EU.”

Svar:

1. Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

> ”Der er ikke sket en ændring af de relevante regler i databeskyttelsesforordningen og databeskyttelsesloven, således som de er nærmere beskrevet i afsnit 1 i besvarelsen af 15. juni 2021 til spørgsmål nr. 316 (Alm. del) fra Folketingets Kulturudvalg.
>
> Datatilsynet kan imidlertid oplyse, at tilsynet ved to tidligere lejligheder har taget stilling til anvendelsen af ansigtsgenkendelse i forbindelse med medlemmers adgang til fitnesscentre.
>
> I den første sag[1] fandt Datatilsynet, at behandlingen kunne ske på baggrund af samtykke. Ansigtsgenkendelsessystemet fungerede ved, at fitnesscentret havde opsat et kamera ved indgangen til centret. Kameraet kunne scanne ansigt på kunder og ansatte, hvorefter resultatet blev holdt op mod billeder allerede uploadet i systemet. Kameraet var imidlertid altid online og blev derfor anvendt uafbrudt. Der skete på denne måde en flygtig og kortvarig behandling af alle personer inden for kameraets synsvidde. Kameraet blev derfor også anvendt på personer, som ikke havde samtykket til den pågældende behandling. Tilsynet fandt, at dette var i uoverensstemmelse med reglerne.

[1] Datatilsynets afgørelse kan finde på tilsynets hjemmeside: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse

Den anden sag[2] omhandlede særligt kravene til samtykke, herunder om de mulige alternativer, som det pågældende fitnesscenter havde udbudt, kunne anses for at udgøre reelle alternativer. I den konkrete sag havde fitnesscentret oplyst klageren, at hvis klageren ikke ønskede at give samtykke til ansigtsgenkendelse, havde klageren kun mulighed for at træne i centrets bemandede åbningstid. Datatilsynet vurderede, at dette medførte, at der ikke var nogen alternativer til samtykke. Dette betød, at det samtykke, fitnesscentret forsøgte at indhente, ikke kunne anses for gyldigt.

Børn har en særlig beskyttelse efter databeskyttelsesforordningen, fordi de er mindre bevidste om de risici og konsekvenser, der kan være forbundet med behandling af personoplysninger. Hertil kommer, at ansigtsgenkendelse kan være en meget indgribende behandling.

Det afhænger af en konkret modenhedsvurdering, om barnet selv kan give samtykke til behandling af oplysninger om barnet. Den dataansvarlige skal derfor konkret vurdere, om barnet har tilstrækkelig modenhed og forståelse til selv at give samtykke. Normalt vil et barn på 15 år være tilstrækkelig moden til at kunne give samtykke på egne vegne.

I modenhedsvurderingen af barnet skal den dataansvarlige lægge særlig vægt på, om barnet har en tilstrækkelig forståelse af rækkevidden af ansigtsgenkendelsen. Hvis den dataansvarlige vurderer, at barnet ikke har den tilstrækkelige modenhed, skal samtykket i stedet indhentes fra en forældremyndighedsindehaver.

Den information, som skal gives forud for meddelelse af samtykke, skal desuden tilpasses barnets forståelse. Informationen skal være formuleret i et klart og let forståeligt sprog, så barnet kan overskue oplysningerne.

Datatilsynet bemærker videre, at enhver risiko, der indebærer en høj konsekvens for de registreredes rettigheder og frihedsrettigheder – også ved relativt lave sandsynligheder for, at risikoen
realiseres – sandsynligvis vil indebære en høj risiko for de registreredes rettigheder, hvilket udløser pligten til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, jf. databeskyttelsesforordningens artikel 35, stk. 1.

[2] Datatilsynets afgørelse kan findes på tilsynets hjemmeside: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/aug/samtykke-til-ansigtsgenkendelse-i-fitnesscenter-var-gyldigt

> I Artikel 29-gruppens (nu Det Europæiske Databeskyttelsesråd, EDPB) retningslinjer om konsekvensanalyse vedrørende databeskyttelse[3] er der fastsat kriterier, der kan hjælpe til at identificere de behandlinger, der vil kræve en konsekvensanalyse. Det følger af retningslinjerne, at en dataansvarlig i de fleste tilfælde kan antage, at en behandling, der opfylder to af kriterierne, skal gøres til genstand for en konsekvensanalyse vedrørende databeskyttelse.
>
> Behandlingen af personoplysninger som led i ansigtsgenkendelse af børn vil opfylde mindst to af disse kriterier, idet der behandles følsomme personoplysninger om sårbare registrerede. Der skal på den baggrund foretages en konsekvensanalyse forud for behandlingen.
>
> Datatilsynet bemærker afslutningsvis, at den dataansvarlige i øvrigt skal sikre overholdelsen af de databeskyttelsesretlige principper i artikel 5 og resten af forordningen, herunder i forbindelse med systemets design, jf. databeskyttelsesforordningens artikel 25."

2. For så vidt angår brugen af biometrisk data til entydig identifikation (som f.eks. ansigtsgenkendelse) er det muligt at fastsætte supplerende regler nationalt inden for rammerne af databeskyttelsesforordningen. Det følger af artikel 9, stk. 4, at medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af bl.a. biometrisk data. Rækkevidden af dette nationale råderum er beskrevet nærmere i Justitsministeriets betænkning nr. 1565 om databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning, punkt 3.9.3., hvor følgende bl.a. fremgår:

> "Med databeskyttelsesforordningens artikel 9, stk. 4, fremhæves det, at der er et videre rum for nationale regler, for så vidt angår disse særligt oplistede personoplysninger.
>
> Efter databeskyttelsesforordningens artikel 9, stk. 4, ses der således at være en relativt stor manøvremargin for medlemsstaterne til at opretholde eller indføre yderligere betingelser, herunder begrænsninger.
>
> Med *betingelser* må der i denne sammenhæng forstås såvel, at medlemsstaterne nationalt kan fastsætte yderligere krav til, hvornår en behandling er lovlig og til, hvilke foranstaltninger

[3] Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP248 rev. 01, vedtaget den 4. april 2017, som senest revideret og vedtaget den 4. oktober 2017.

der skal iagttages som led i en given behandling. En medlemsstat vil således – inden for bestemmelsens rammer – have adgang til f.eks. at fastsætte, at en behandling af helbredsoplysninger skal ske på en særlig måde (f.eks. elektronisk), omfatte særlige oplysninger (f.eks. diagnose og sygdomshistorik) og indebære videregivelse til nærmere fastsatte modtagere.

Muligheden for at opretholde eller indføre yderligere betingelser, herunder begrænsninger, er dog begrænset af, at det ikke bør hæmme den frie udveksling af personoplysninger i EU, når disse betingelser finder anvendelse på grænseoverskridende behandling af sådanne oplysninger. Dette krav må i praksis navnlig antages at have relevans for regulering, der direkte er rettet mod den private sektor, eller i væsentlig grad påvirker denne, idet hensynet til den fri bevægelighed må antages i praksis at have mere begrænset betydning for den offentlige sektor. Dog vil ethvert relevant lovgivningsmæssigt tiltag mv. skulle vurderes i forhold til dette krav, uanset om det er rettet mod den private eller offentlige sektor.

Dette krav ses netop at underbygge, at medlemsstaterne – udover ved grænseoverskridende behandling – har et ganske vidt spillerum for at fastsætte nationale særregler."